IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF APPLE IPHONE XR IMEI NUMBER 356423101378701O, BELIEVED TO BE CURRENTLY LOCATED AT 150 TOWN SQUARE CIRCLE, #208, MOORESVILLE, NC	Case No. 3:20-mj-309

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent Jennifer Howell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a Search Warrant authorizing the examination of property—an electronic device— believed to be currently located at 150 Town Square Circle, #208 Mooresville, NC, and the extraction from that property of electronically stored information described in Attachment B.

2. I, Jennifer Howell, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been since February 2005. I am currently assigned to the Child Exploitation/Human Trafficking Task Force at the Charlotte Division of the FBI. In my current capacity, I am assigned to investigate federal crimes against children to include child pornography, on-line enticement, international parental kidnapping, child abductions, sexual exploitation of children, domestic trafficking of children and adults/prostitution, child sex

tourism, and national sex offender registry violations. I have received extensive training in investigations as a New Agent Trainee at the FBI Academy in Quantico, Virginia. My training has continued through in-service training seminars during my assignment as an FBI Special Agent. I have also participated in ordinary methods of investigation, including but not limited to, consensual monitoring, physical surveillance, interviews of witnesses and subjects, the use of confidential informants, pen registers, and Title III court ordered interceptions. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws and I am authorized by the Attorney General to request a Search Warrant.

3. The statements contained in this Affidavit are based on my experience and background as a law enforcement officer and on information provided by other law enforcement agents and other organizations. This Affidavit is intended to show only that there is sufficient probable cause for the requested Warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone XR with phone number #704-705-0526, hereinafter the "Device." The Device is currently located at 150 Town Square Circle, #208, Mooresville, NC 28117 and will be transported to the FBI Charlotte Division located at 7915 Microsoft Way, Charlotte, North Carolina.

5. The applied-for Warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

1. The United States, including the Federal Bureau of Investigation (FBI), is conducting a criminal investigation of **MARK VAN EPERN** regarding a possible violation of 18 U.S.C. § 1512(b).

2. FBI Charlotte opened a federal investigation based on information provided by Huntersville Police Department (HPD) in reference to MARK VAN EPERN (VAN EPERN) who attempted to produce child pornography.

3. A FBI WITNESS who has produced evidence in the case against VAN EPERN has received a threat from VAN EPERN who is now aware of her involvement with the FBI.

4. The WITNESS stated that on September 08, 2020, VAN EPERN threatened that he would kill her if he found out that she gave the FBI a phone he bought in January 2019. VAN EPERN said he would kill her if she gave it to the FBI and if she communicated with the FBI. He said he would stab her in the chest and he has access to his friend's guns.

5. On October 13, 2020, the WITNESS was interviewed at the U.S. Attorney's Office to discuss the details of her threat from VAN EPERN. The WITNESS stated she spoke to VAN EPERN on the phone the weekend prior to Labor Day in September 2020. VAN EPERN stated he wanted a package that was mailed to her house and to pick up his clothes and other personal belongings. During the conversation, VAN EPERN mentioned the words poisoning himself and the WITNESS. The package arrived at the WITNESS's house sometime in mid-August and she is unsure if the postman dropped it off or if VAN EPERN dropped it off in order to bait her to see him. VAN EPERN's forwarding address was on the package, so the WITNESS is unsure as to why the package would have been delivered to her house. On September 08, 2020, the

WITNESS delivered the package to VAN EPERN at his residence. During the course of the conversation, VAN EPERN said she better not talk to the FBI and that he knows she has already been talking to the FBI. VAN EPERN threatened to kill her if she gave a phone to the FBI that belonged to him and if she continued to talk to the FBI. VAN EPERN mentioned a gun and killing her and himself. VAN EPERN doesn't currently own a gun but could get access to one through friends.

6. The WITNESS stated that VAN EPERN previously tried to hurt himself around 2018 when he cut himself in the neck and torso and was hospitalized. In 2013, VAN EPERN broke the WITNESS's arm when he grabbed her wrists in order to get a cell phone out of her hands. The WITNESS believes that VAN EPERN will hurt himself again and also the WITNESS.

7. In order to help verify that the threats from VAN EPERN to the WITNESS occurred around September 08, 2020, as well as to verify the order history of the package and proof of delivery of the package, your Affiant is requesting a search of the device. It is common for individuals to keep their cell phones in their residence so your Affiant is also requesting a search of the residence in order to locate the device.

8. On October 13, 2020, your Affiant requested an exigent request from AT&T and on October 21, 2020 submitted an administrative subpoena to confirm subscriber information for phone number #704-705-0526. AT&T responded that the phone is an Apple iPhone XR, the IMEI number is 356423101378701O, and the subscriber is MARK VAN EPERN. The address associated with the account is 150 Town Square Circle, #208, Mooresville, NC and VAN EPERN has been the subscriber since November 2018.

9. VAN EPERN and the WITNESS have communicated periodically using

their cell phone for voice and text messaging. Also, it is common for postal service mail carriers to send texts, emails, and photographs to cell phones in order to confirm orders, shipments, and delivery of packages. Cell phones, such as the iPhone XR subscribed to by the defendant are capable of receiving and storing large amounts of photographs, emails, texts, and other information for long periods of time, if not indefinitely.

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system ("GPS") technology for determining the location of the device.

b. "Computer," as used herein, is defined pursuant to 18 U.S. C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

c. Laptop: Laptop computers, also known as notebooks, are portable computers that can operate in a wide range of environments due to their portability. Because laptops are meant to be portable, they have a battery which allows them to operate without being plugged into a power outlet.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected

to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

12. There is probable cause to believe that items which were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, cellular device storage media—in particular, computers' internal hard drives—contain electronic evidence of how a cellular device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Cellular device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

13. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the Warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of external storage media and the times a cellular device was in use. Cellular device file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a cellular device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a Search Warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cellular device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the Warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses a cellular device to receive, store or send child pornography, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a cellular device used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; and other records that indicate the nature of the offense.

14. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the Warrant I am applying for would permit the examination of the device consistent with the Warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the Warrant.

CONCLUSION

15. I submit that this Affidavit supports probable cause for a Search Warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully Submitted,

_/s/ Jennifer Howell_____
Jennifer Howell, Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 23rd day of October, 2020, at 2:26 PM

Signed: October 23, 2020

David S. Cayer
United States Magistrate Judge

ATTACHMENT A

1. The property to be searched is an Apple iPhone XR with phone number #704-705-0526, IMEI number 3564231013787010, hereinafter the "Device." The Device is currently believed to be located at 150 Town Square Circle, #208, Mooresville, North Carolina 28117 and will be transported to the FBI Charlotte Division located at 7915 Microsoft Way, Charlotte, North Carolina.

This Warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

During the execution of the search of the Device described in Attachment A, law enforcement personnel are authorized to search and seize the following:

1. All records relating to violations of 18 U.S.C. § 1512(b), makes it a crime for any person who knowingly uses intimidation, threatens, or corruptly persuades another person, or attempts to do so, or engages in misleading conduct toward another person, with intent to (1)influence, delay, or prevent the testimony of any person in an official proceeding; (2)cause or induce any person to (A) withhold testimony, or withhold a record, document, or other object, from an official proceeding; (B) alter, destroy, mutilate, or conceal an object with intent to impair the object's integrity or availability for use in an official proceeding; (C) evade legal process summoning that person to appear as a witness, or to produce a record, document, or other object, in an official proceeding; or (D) be absent from an official proceeding to which such person has been summoned by legal process, involving VAN EPERN.

2. Documents or files showing communication between VAN EPERN and the WITNESS including any e-mails, texts, images, photographs, videos, and chat logs.

3. Any and all emails, texts, phone calls and other information relating to package orders, shipping confirmations, delivery, delivery receipt, address confirmation, address changes and address forwarding history.

4. Any and all photographs exchanged between VAN EPERN and the WITNESS, as well as any and all photographs of the package to include package history and confirmation receipts.

5. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence.

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device.

7. Evidence of who used, owned, or controlled the Device during the time period and activities described in this Warrant were occurring such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant message logs, photographs, and correspondence.

8. Evidence of the dates and times the Device was used during the activities described in this Warrant.

9. Records of or information about Internet Protocol addresses accessed by the Device, including routers, modems, and network equipment used to connect the Device to the Internet and internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

10. Any and all records, notes, documents, invoices, and materials, including digital data files, that concern online storage, including but not limited to software used to access such online storage, user logs, or archived data that show connection to such online storage, and user logins and passwords for such online storage.

11. Evidence indicating how and when the Device was accessed or used to determine the chronological context of the access, use, and events relating to crime under investigation and to the Device user;

12. Evidence indicating the Device user's state of mind as it relates to the crime under investigation;

13. Passwords, encryption keys, and other access devices that may be necessary to access the Device;

14. Contextual information necessary to understand the evidence described in this attachment.

15. Records of or information about who owned the Device at the time the things described in this Warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

16. This Warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this Warrant in order to locate evidence, fruits, and instrumentalities described in this Warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this Warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

17. If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e.

communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.